配置WLC和ACS以对管理用户进行身份验证

目录

简介

本文档介绍如何配置WLC和Cisco Secure ACS，以便AAA服务器可以对控制器上的管理用户进行身份验证。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 了解如何在WLC上配置基本参数
- 了解如何配置RADIUS服务器（如Cisco Secure ACS）

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行版本7.0.216.0的Cisco 4400无线局域网控制器
- 运行软件版本4.1且在此配置中用作RADIUS服务器的Cisco Secure ACS。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

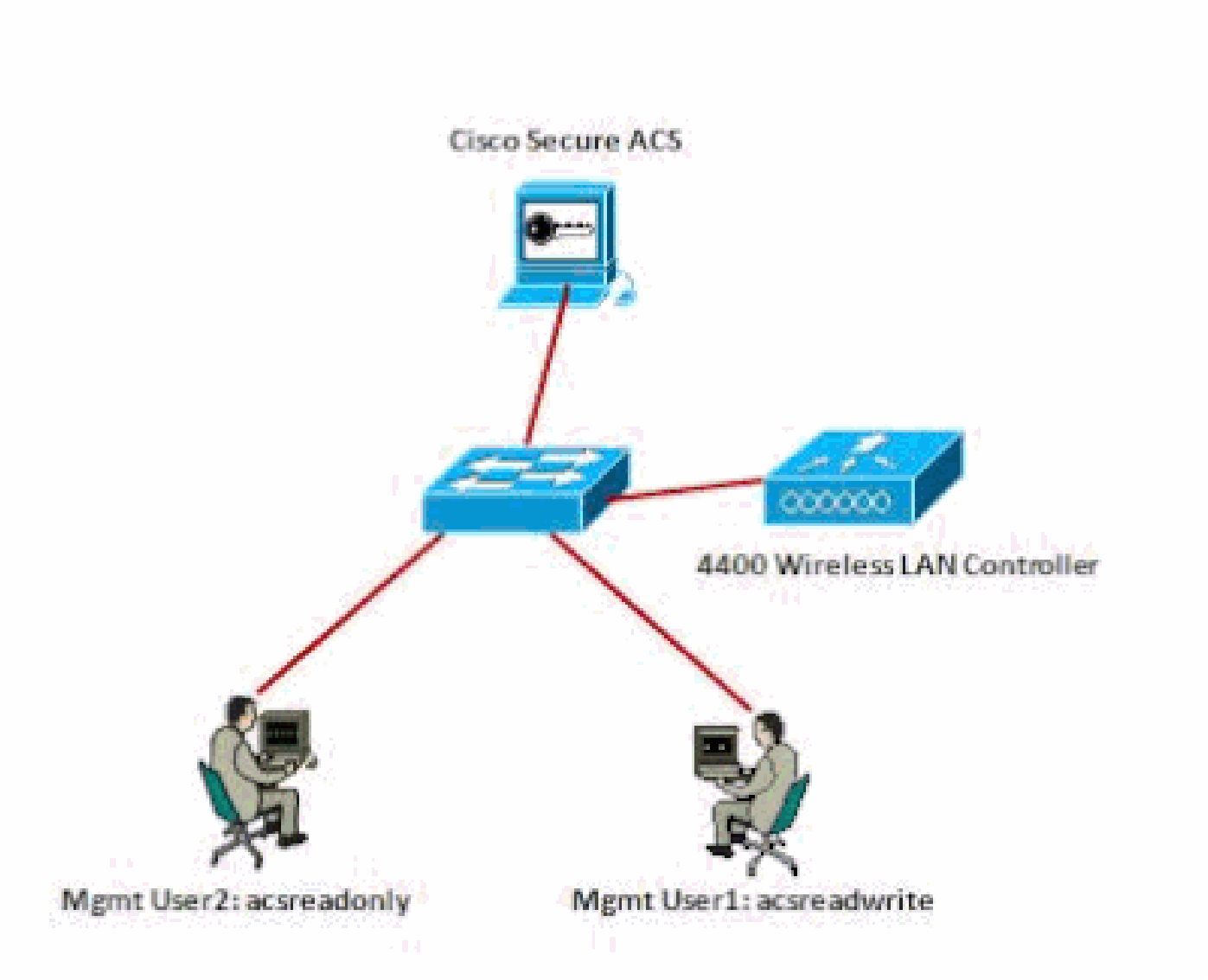
本文档说明如何配置无线LAN控制器(WLC)和访问控制服务器(Cisco Secure ACS)，以便身份验证、授权和记帐(AAA)服务器可以对控制器上的管理用户进行身份验证。本文档还说明了不同的管理用户如何通过从Cisco Secure ACS RADIUS服务器返回的供应商特定属性(VSA)获得不同的权限。

配置

本部分提供有关如何配置WLC和ACS的信息，以实现本文档中介绍的目的。

网络图

本文档使用以下网络设置：



网络图

此配置示例使用以下参数：

- Cisco Secure ACS的IP地址— 172.16.1.1/255.255.0.0
- 控制器的管理接口IP地址— 172.16.1.30/255.255.0.0
- 在接入点(AP)和RADIUS服务器上使用的共享密钥- asdf1234
- 以下是该示例在ACS上配置的两名用户的凭证：
    - 用户名- acsreadwrite

      密码- acsreadwrite
    - 用户名- acsreadonly

      密码- acsreadonly

您需要配置WLC和Cisco Secure Cisco Secure ACS以便：

- 使用用户名和口令acsreadwrite登录到WLC的所有用户都获得对WLC的完全管理访问权限。
- 使用用户名和口令acsreadonly登录到WLC的所有用户都获得对WLC的只读访问权限。

配置

本文档使用以下配置：

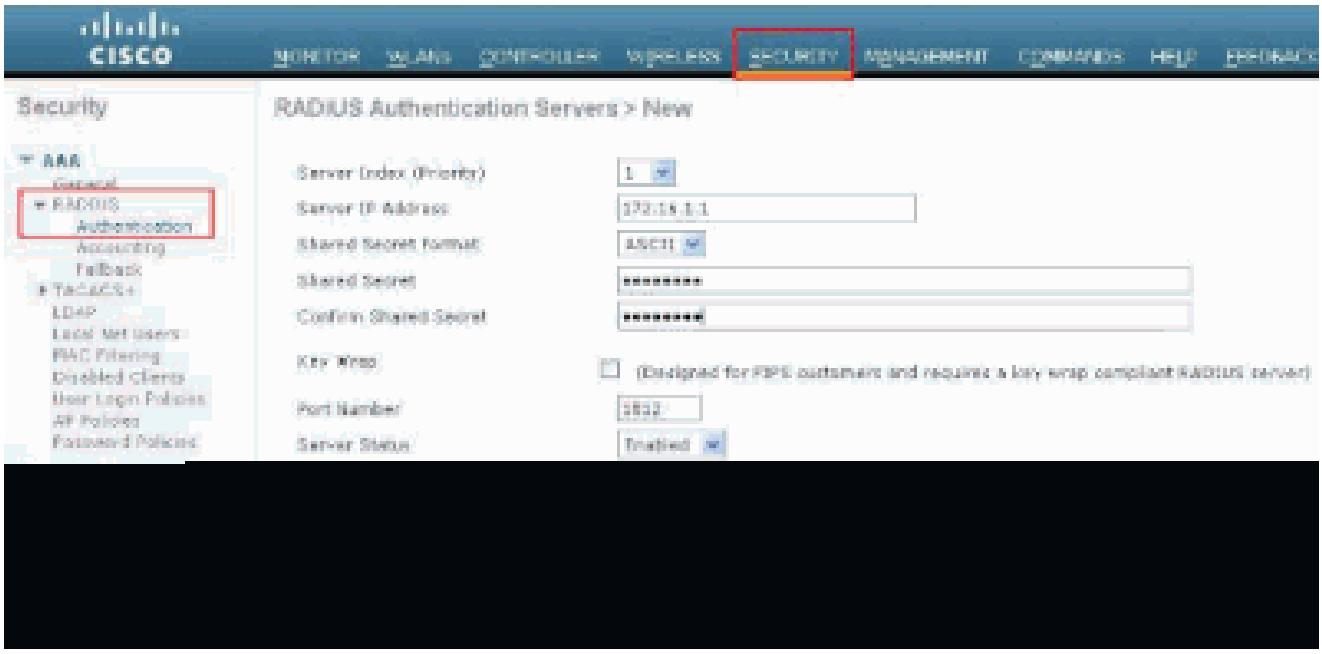
- WLC 配置
- Cisco Secure ACS配置

WLC 配置

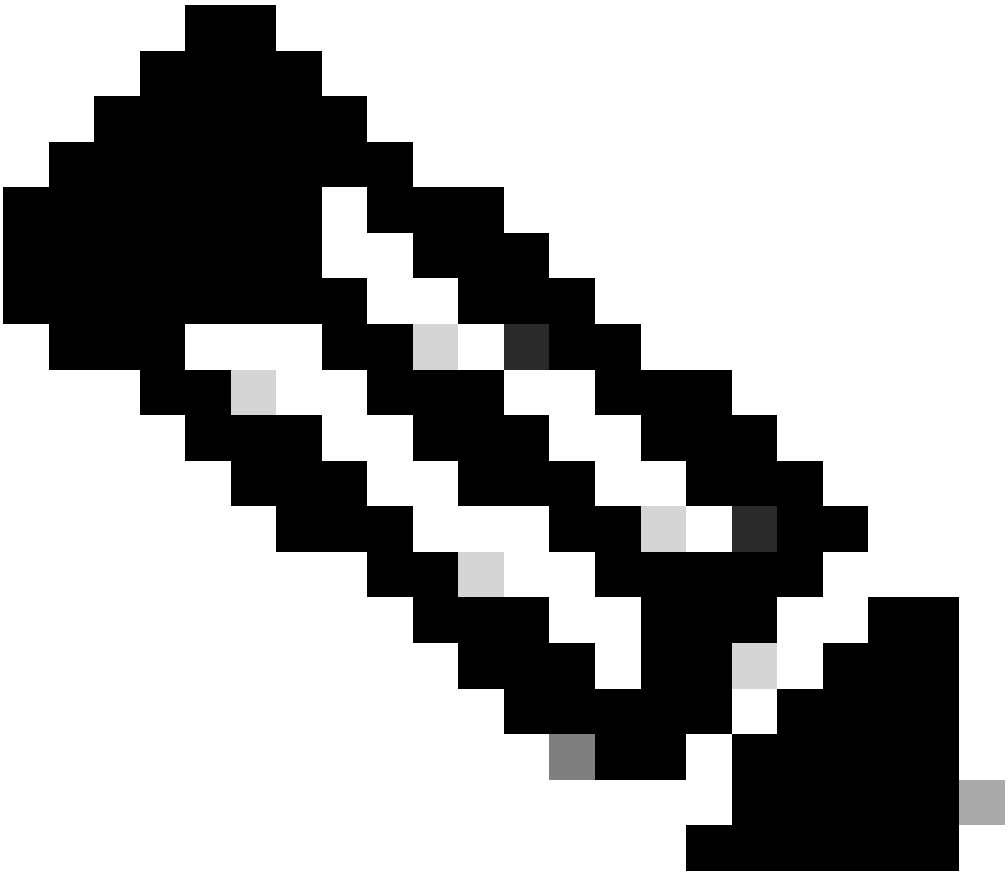
配置WLC以接受通过Cisco Secure ACS服务器进行的管理

完成以下步骤以配置WLC，使其与RADIUS服务器通信：

1. 从 WLC GUI 中，单击 Security。 从左侧的菜单中单击RADIUS > Authentication。 系统将显示RADIUS Authentication servers页面。要添加新的RADIUS服务器，请单击New。在 RADIUS Authentication Servers > New 页中，输入特定于RADIUS服务器的参数。下面是一个示例。

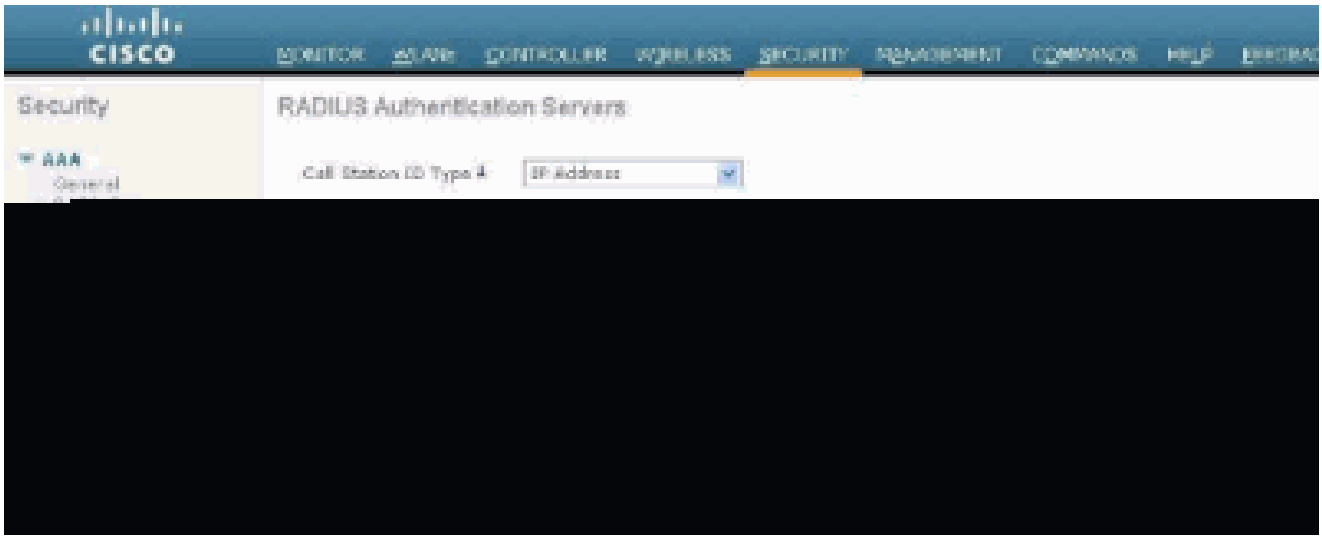


2. 选中Management单选按钮，以便允许RADIUS服务器对登录WLC的用户进行身份验证。



注意：确保此页上配置的共享密钥与RADIUS服务器上配置的共享密钥匹配。只有这样WLC才能与RADIUS服务器通信。

3. 验证是否已将WLC配置为由Cisco Secure ACS管理。为此，请从WLC GUI中单击Security。显示的GUI窗口类似于此示例。



您可以看到为RADIUS服务器172.16.1.1启用了Management复选框。这说明允许ACS对WLC上的管理用户进行身份验证。

Cisco Secure ACS配置

要配置ACS，请完成以下部分中的步骤：

1. 将WLC作为AAA客户端添加到RADIUS服务器。
2. 配置用户及其相应的RADIUS IETF属性。
3. 配置具有读写访问权限的用户。
4. 配置具有只读访问权限的用户。

将WLC作为AAA客户端添加到RADIUS服务器

要在Cisco Secure ACS中将WLC添加为AAA客户端，请完成以下步骤：

1. 从 ACS GUI 中，单击 Network Configuration。
2. 在 AAA Clients 下，单击 Add Entry。
3. 在Add AAA Client窗口中，输入WLC主机名、WLC的IP地址和共享密钥。

   在本示例中，设置如下：

   - AAA客户端主机名为WLC-4400
   - 172.16.1.30/16是AAA客户端IP地址，在本例中为WLC。
   - 共享密钥是“asdf1234”。

添加AAA客户端窗口

此共享密钥必须与您在WLC上配置的共享密钥相同。

4. 从Authenticate Using下拉菜单中，选择RADIUS (Cisco Airespace)。
5. 单击Submit + Restart 以保存配置。

配置用户及其相应的RADIUS IETF属性

要通过RADIUS服务器对用户进行身份验证，对于控制器登录和管理，您必须将具有IETF RADIUS attributeService-Typeset的用户添加到RADIUS数据库，并根据用户权限将用户添加到适当的值。

- 要为用户设置读写权限，请将Service-TypeAttribute设置为Administrative。
- 要为用户设置只读权限，请将Service-TypeAttribute设置为NAS-Prompt。

配置具有读写访问权限的用户

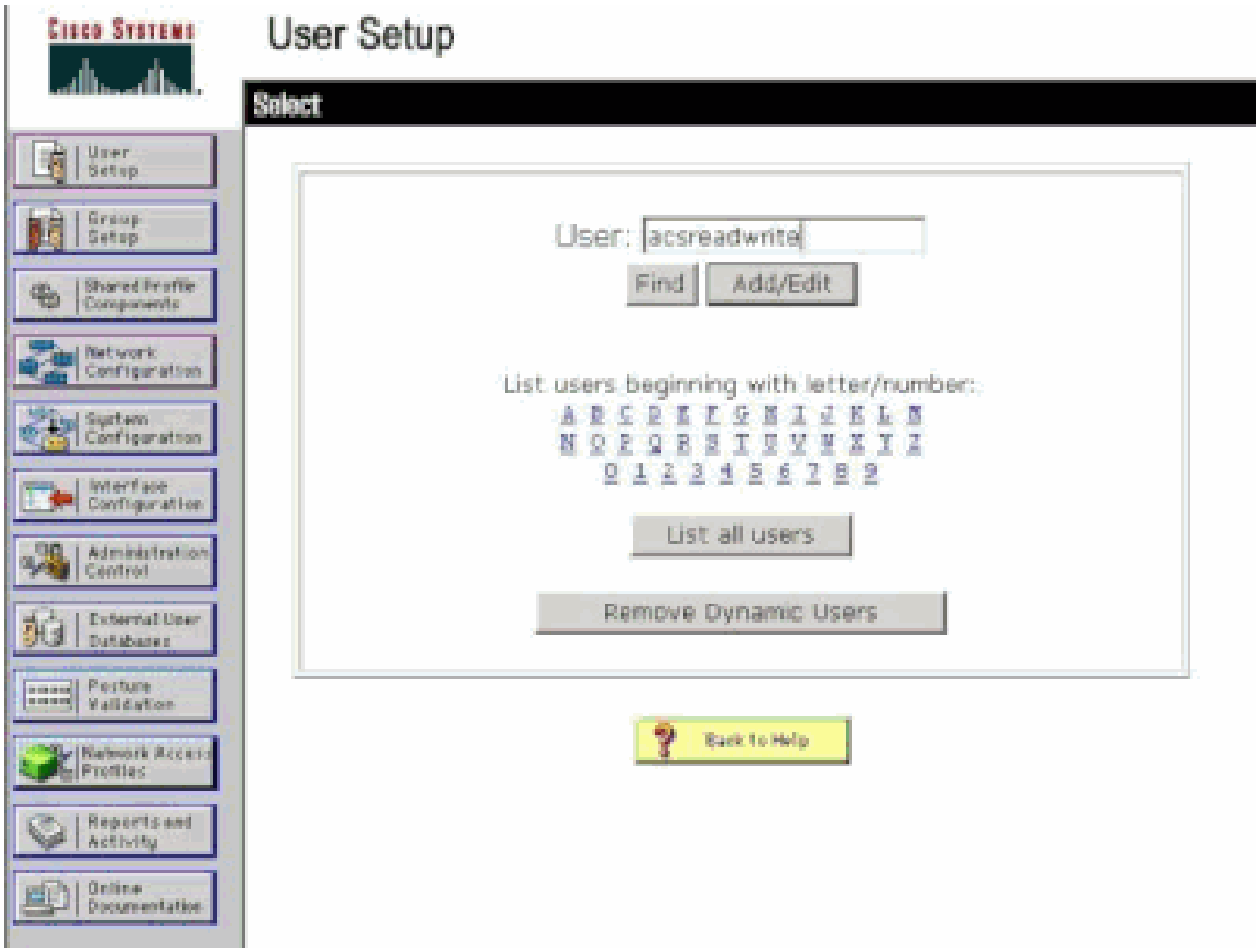
第一个示例显示了具有WLC完全访问权限的用户的配置。当此用户尝试登录控制器时，RADIUS服务器会进行身份验证并向此用户提供完全管理访问权限。

在本示例中，用户名和口令为acsreadwrite。

在Cisco Secure ACS上完成以下步骤。

1. 从 ACS GUI 中，单击 User Setup。

2. 键入要添加到ACS的用户名，如以下示例窗口所示。



用户设置窗口

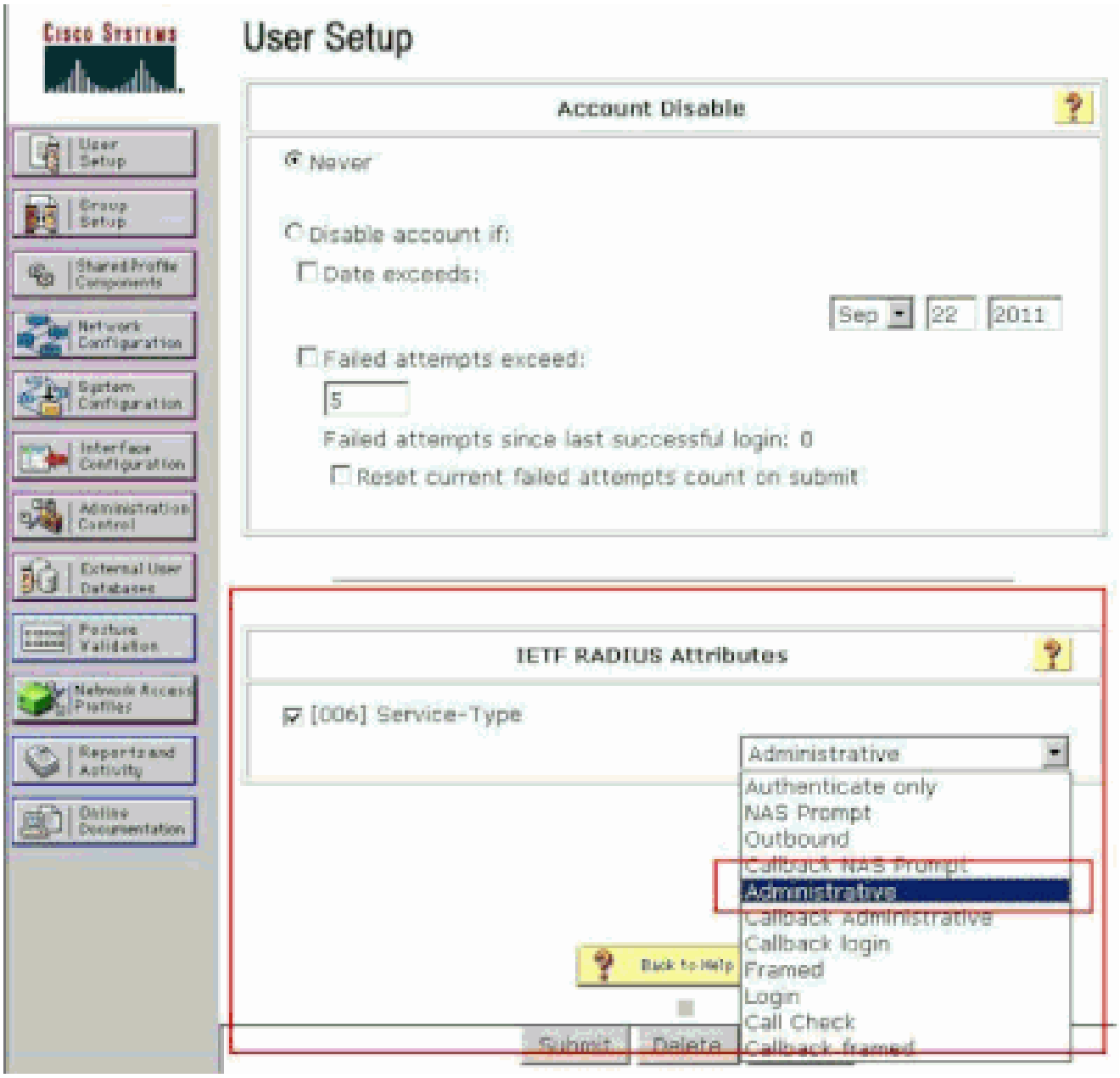
3. 单击Add/Edit转到“User Edit”页。

4. 在“用户编辑”页中，提供此用户的实际名称、说明和密码详细信息。

5. 向下滚动到IETF RADIUS Attributes设置并选中Service-Type Attribute。

6. 因为在本例中，需要为用户acsreadwrite授予完全访问权限，所以请在Service-Type下拉菜单中选择Administrative，然后单击Submit。

   这可确保此特定用户具有对WLC的读写访问权限。



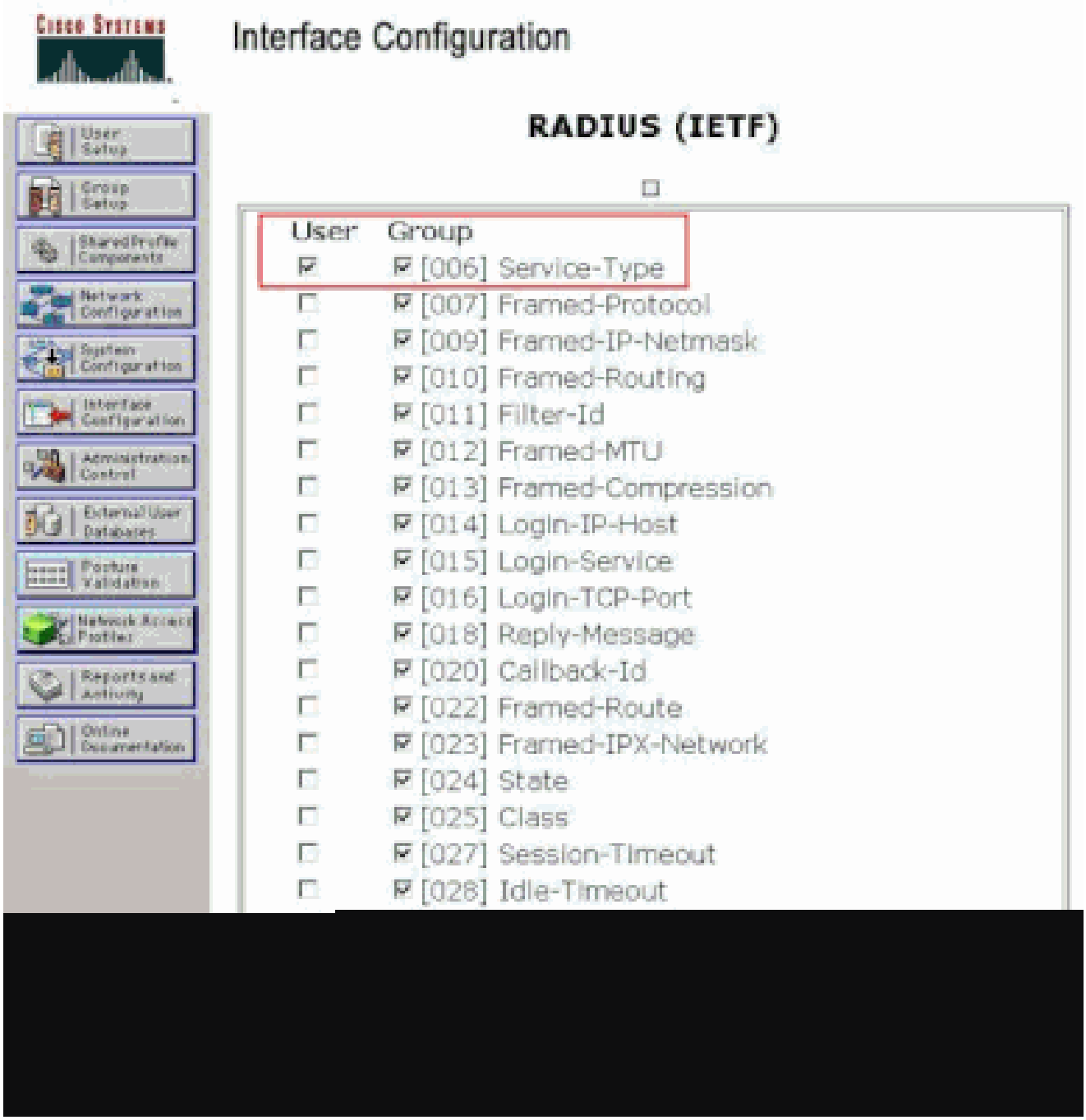
ETF RADIUS属性设置

有时，此Service-Type属性在用户设置下不可见。在这种情况下，请完成以下步骤使其可见。

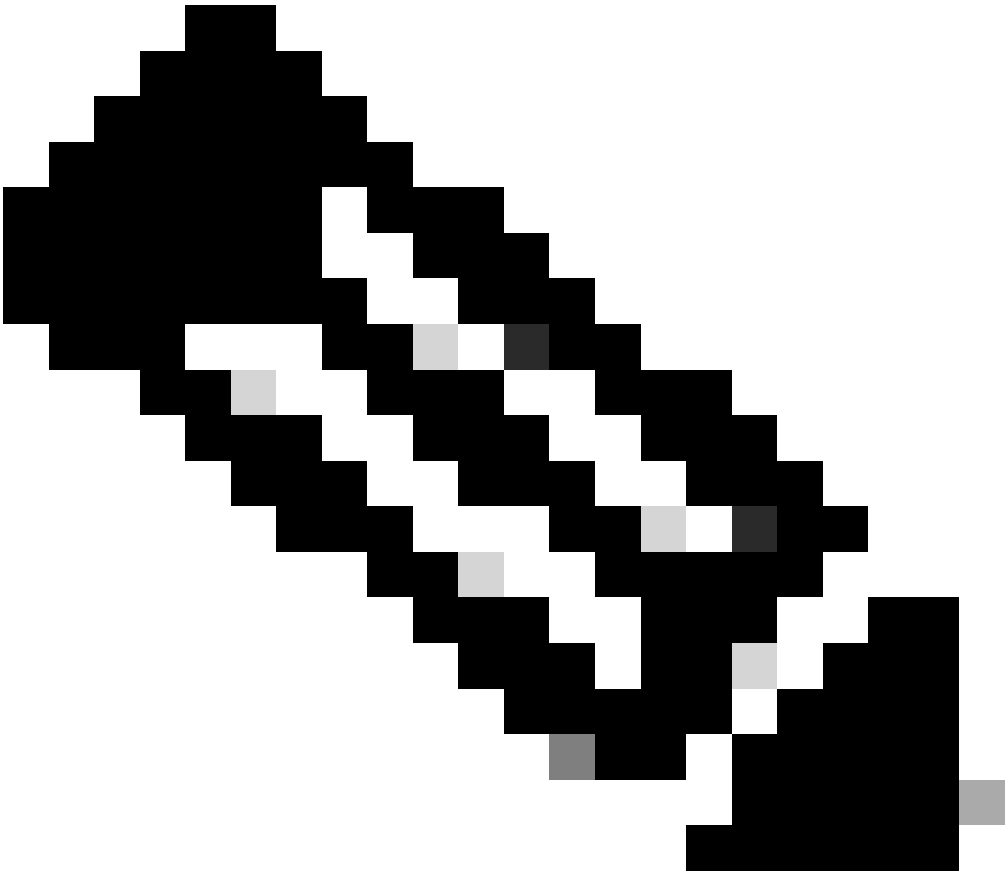
1. 从ACS GUI中，选择Interface Configuration > RADIUS (IETF)以便在User Configuration窗口中启用IETF属性。

   这会将您引导至RADIUS (IETF) Settings页面。

2. 从RADIUS (IETF) Settings页面，您可以启用需要在用户或组设置下可见的IETF属性。对于此配置，请为“User”列选中Service-Type，然后单击Submit。 此窗口显示了一个示例。



RADIUS (IETF)设置页面



注意：此示例指定基于每个用户的身份验证。您还可以根据特定用户所属的组执行身份验证。在这种情况下，请启用Group复选框，以便此属性在Group settings下可见。此外，如果身份验证基于组，您需要将用户分配到特定组，并配置组设置IETF属性，以便为该组的用户提供访问权限。有关如何配置和管理组的详细信息，请参阅组管理。

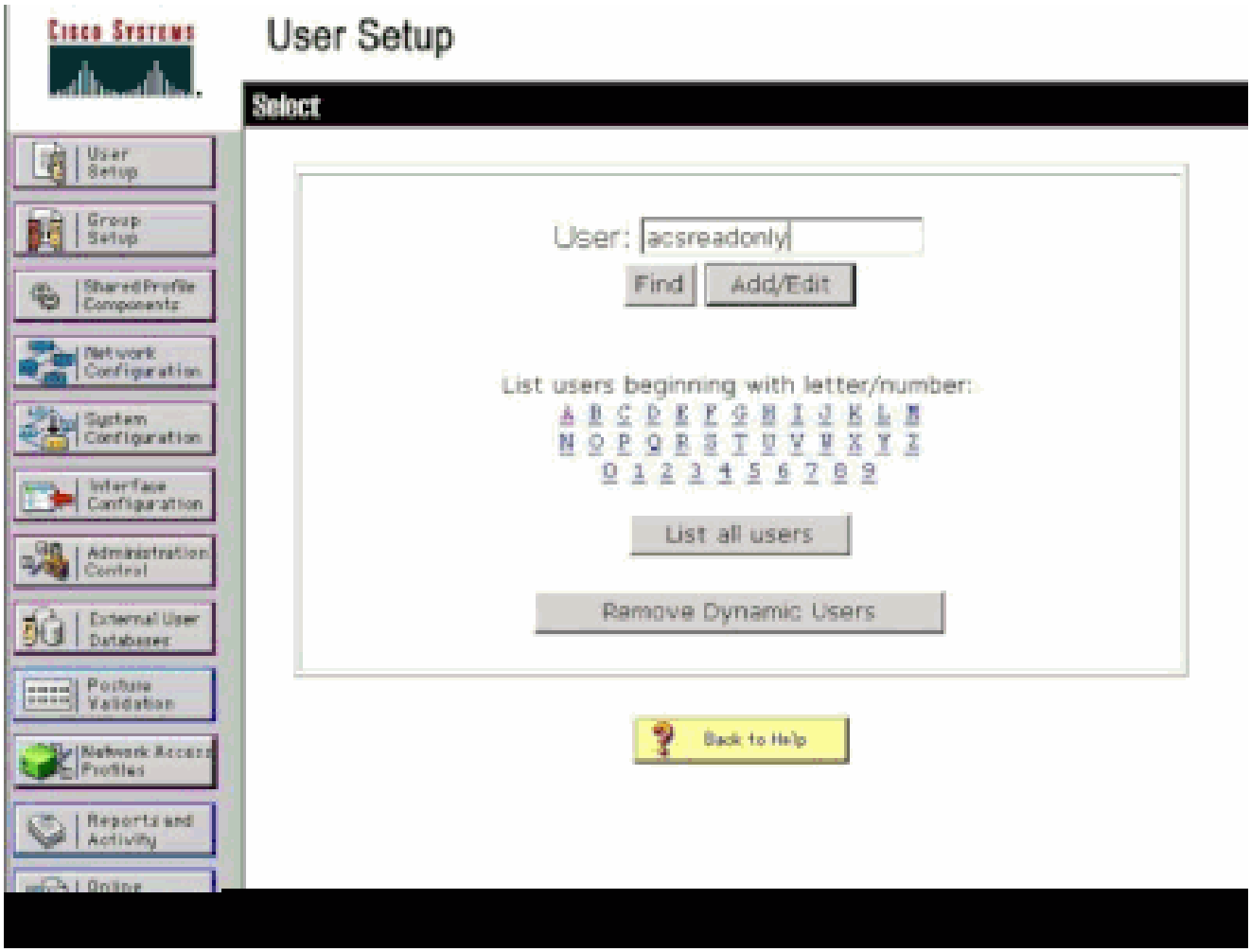
配置具有只读访问权限的用户

此示例显示对WLC具有只读访问权限的用户的配置。当此用户尝试登录控制器时，RADIUS服务器会进行身份验证并向此用户提供只读访问权限。

在本示例中，用户名和口令为acsreadonly。

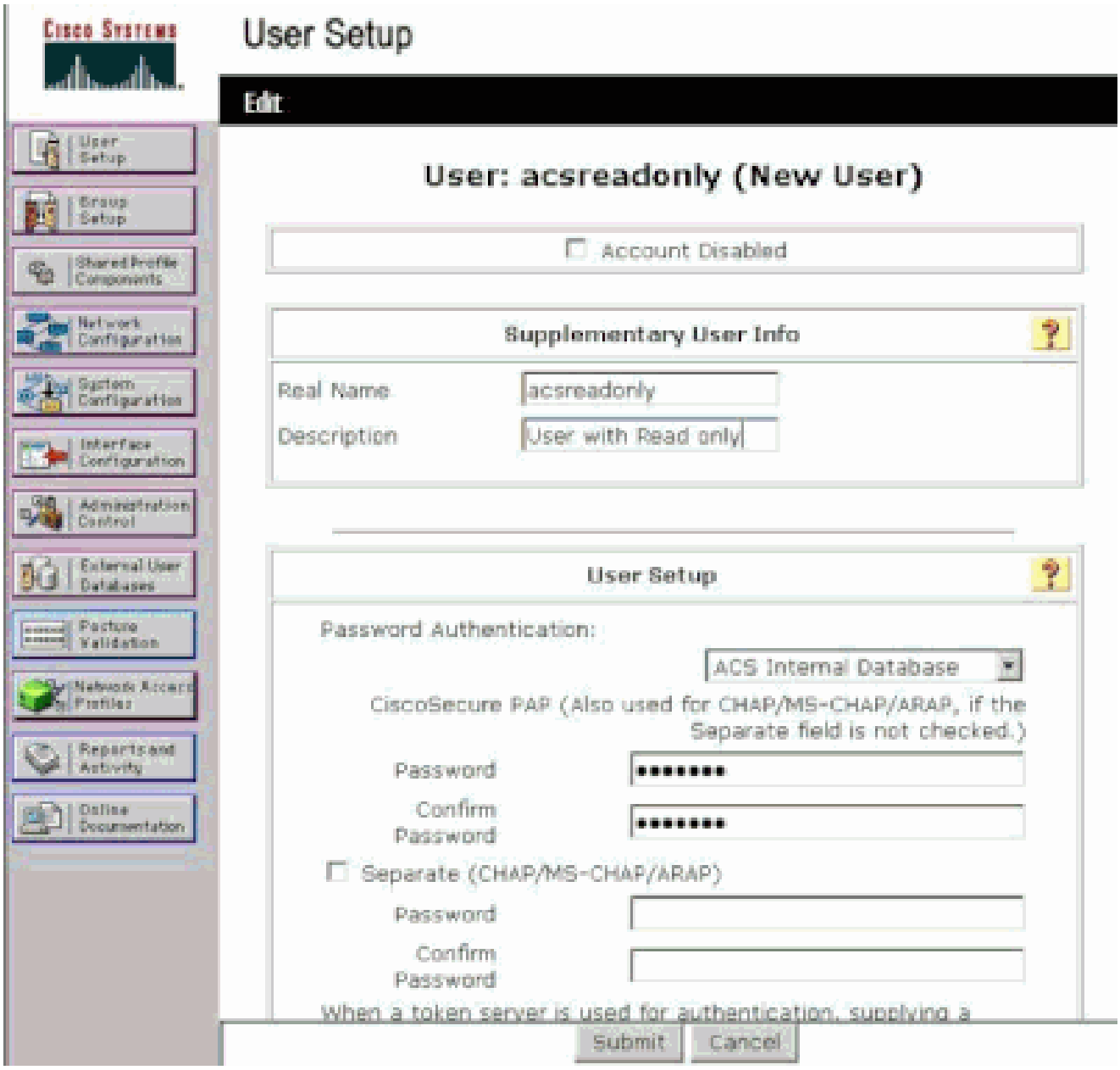
在 Cisco Secure ACS 上完成以下步骤：

1. 从 ACS GUI 中，单击 User Setup。
2. 键入要添加到ACS的用户名，然后单击Add/Edit转到User Edit页。



添加用户名

3. 提供此用户的真实名称、说明和密码。此窗口显示了一个示例。

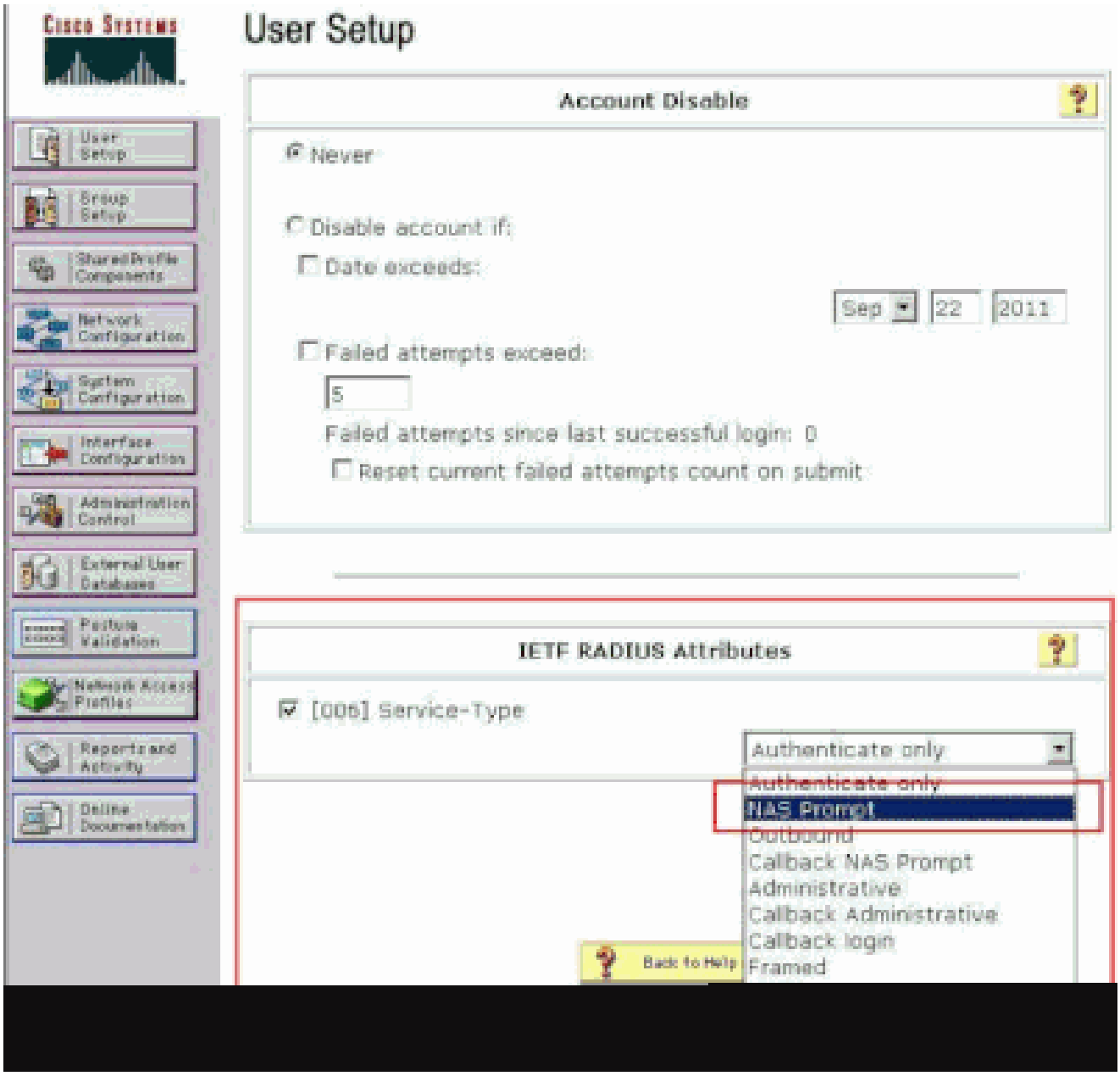


提供已添加用户的真实名称、说明和密码

4. 向下滚动到IETF RADIUS Attributes设置并选中Service-Type Attribute。

5. 由于在本示例中，用户acsreadonly需要具有只读访问权限，请从Service-Type下拉菜单中选择NAS Prompt并单击Submit。

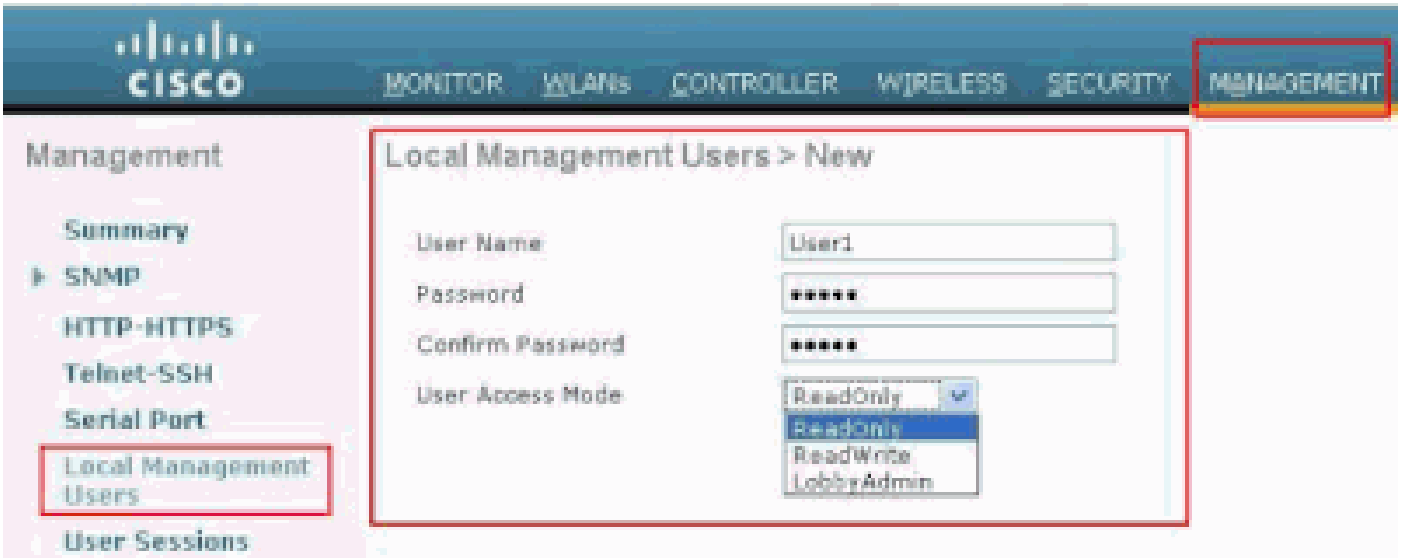
   这可以确保此特定用户对WLC具有只读访问权限。



检查服务类型属性

本地以及通过RADIUS服务器管理WLC

您还可以在WLC上本地配置管理用户。这可以在控制器GUI的Management > Local Management Users下完成。



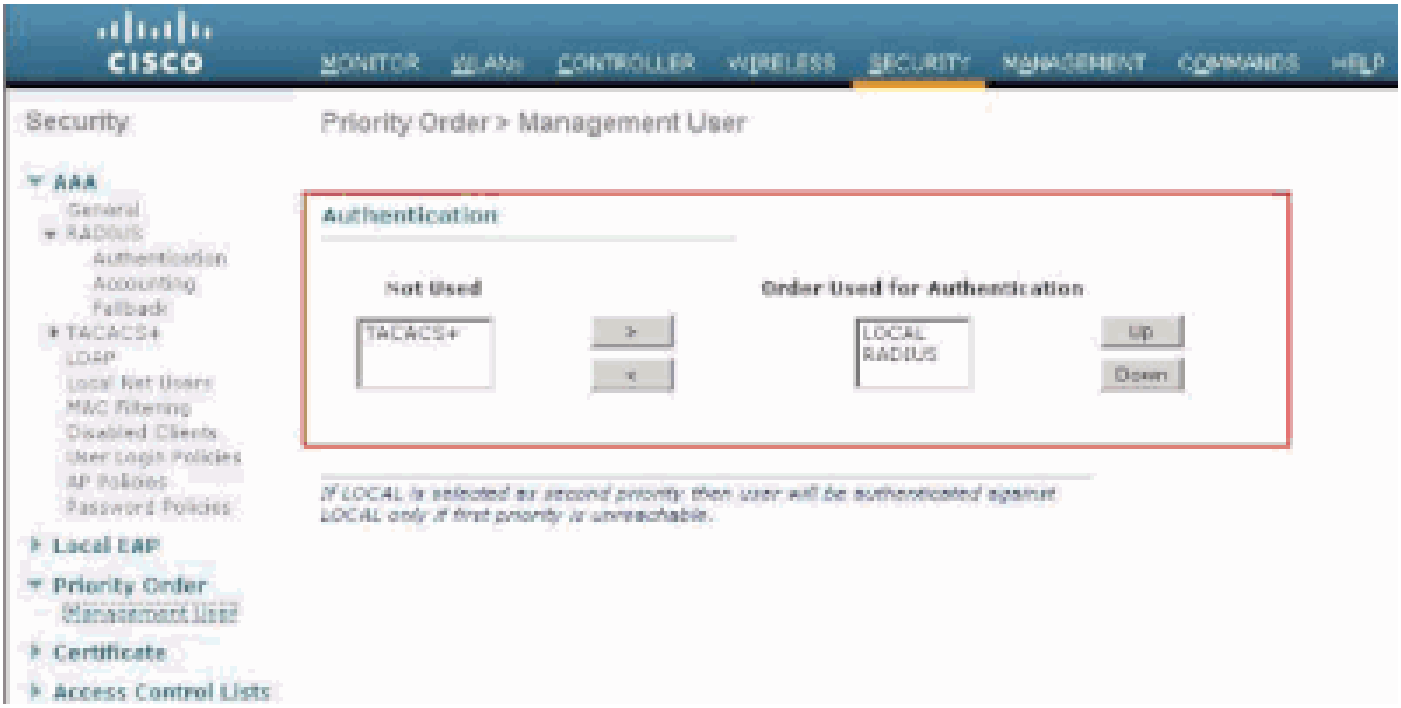
在WLC上本地配置管理用户

假设WLC配置了管理用户（本地以及RADIUS服务器中），并启用了Management复选框。在这种情况下，默认情况下，当用户尝试登录WLC时，WLC的行为方式如下：

1. WLC首先查看为验证用户而定义的本地管理用户。如果该用户存在于其本地列表中，则允许对该用户进行身份验证。如果此用户不在本地显示，则它将查找RADIUS服务器。

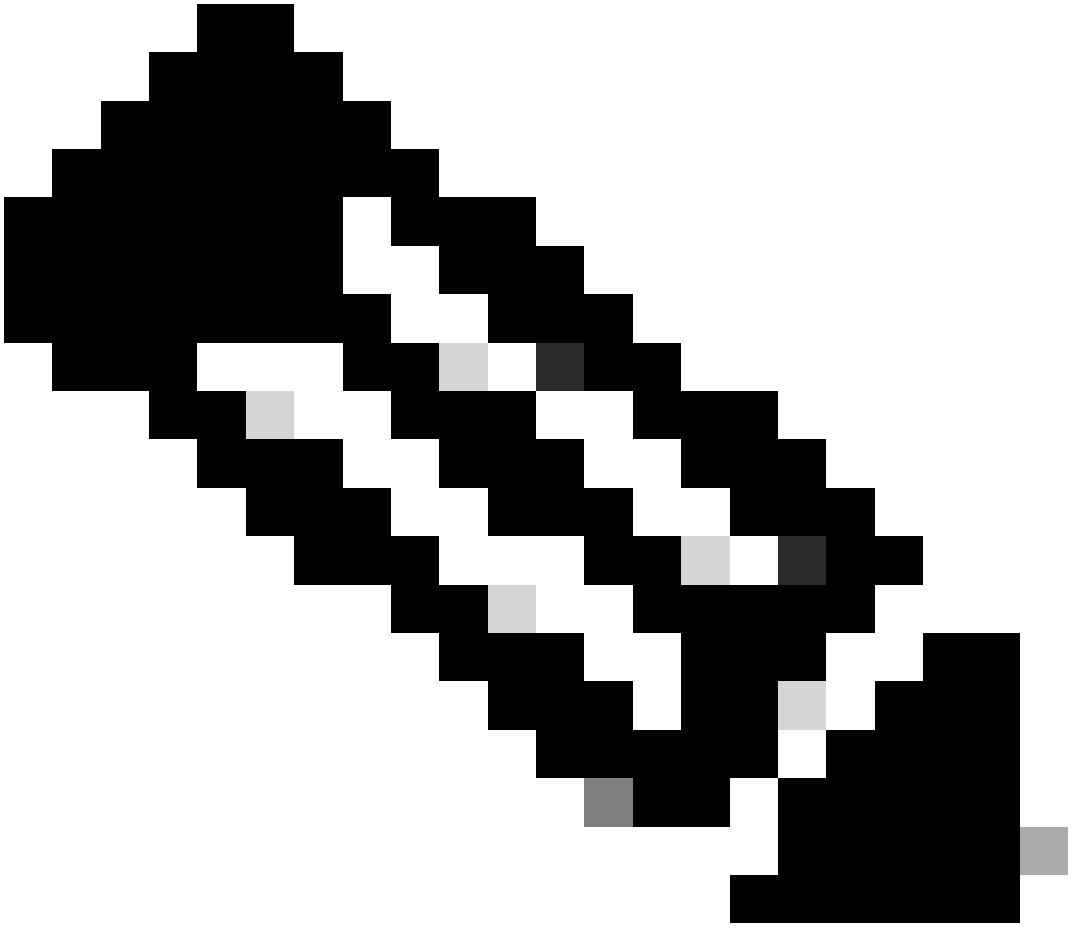
2. 如果同一用户同时存在于本地和RADIUS服务器中，但具有不同的访问权限，则WLC将使用本地指定的权限对用户进行身份验证。换句话说，与RADIUS服务器相比，WLC上的本地配置始终优先。

可以在WLC上更改管理用户的身份验证顺序。为此，请在WLC上的Security页上单击Priority Order > Management User。 在此页面中，您可以指定身份验证的顺序。下面是一个示例。



Management User Selection" />

Priority Order > Management User Selection



注意：如果将LOCAL选为第二优先级，则仅当定义为第一优先级的方法(RADIUS/TACACS)不可达时，才使用此方法验证用户。

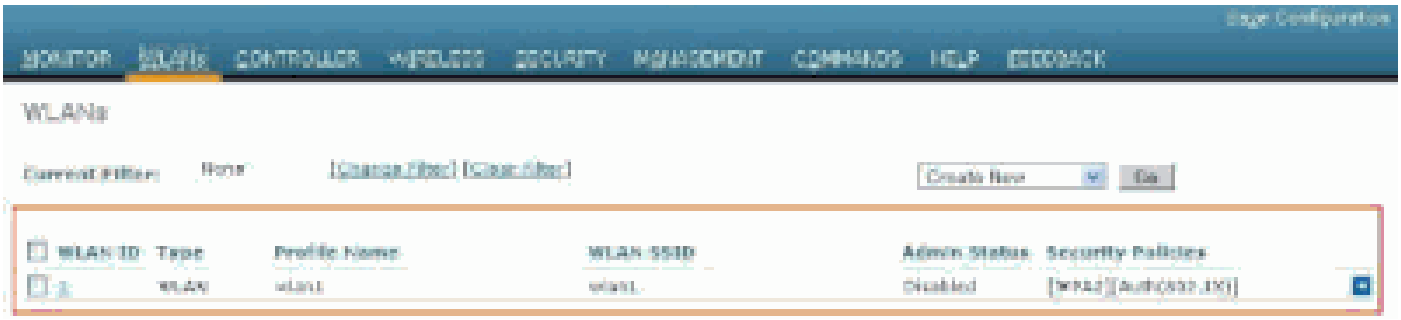
验证

要验证配置是否正常工作，请通过CLI或GUI (HTTP/HTTPS)模式访问WLC。出现登录提示时，键入在Cisco Secure ACS上配置的用户名和密码。

如果配置正确，则表明您已成功在WLC中通过身份验证。

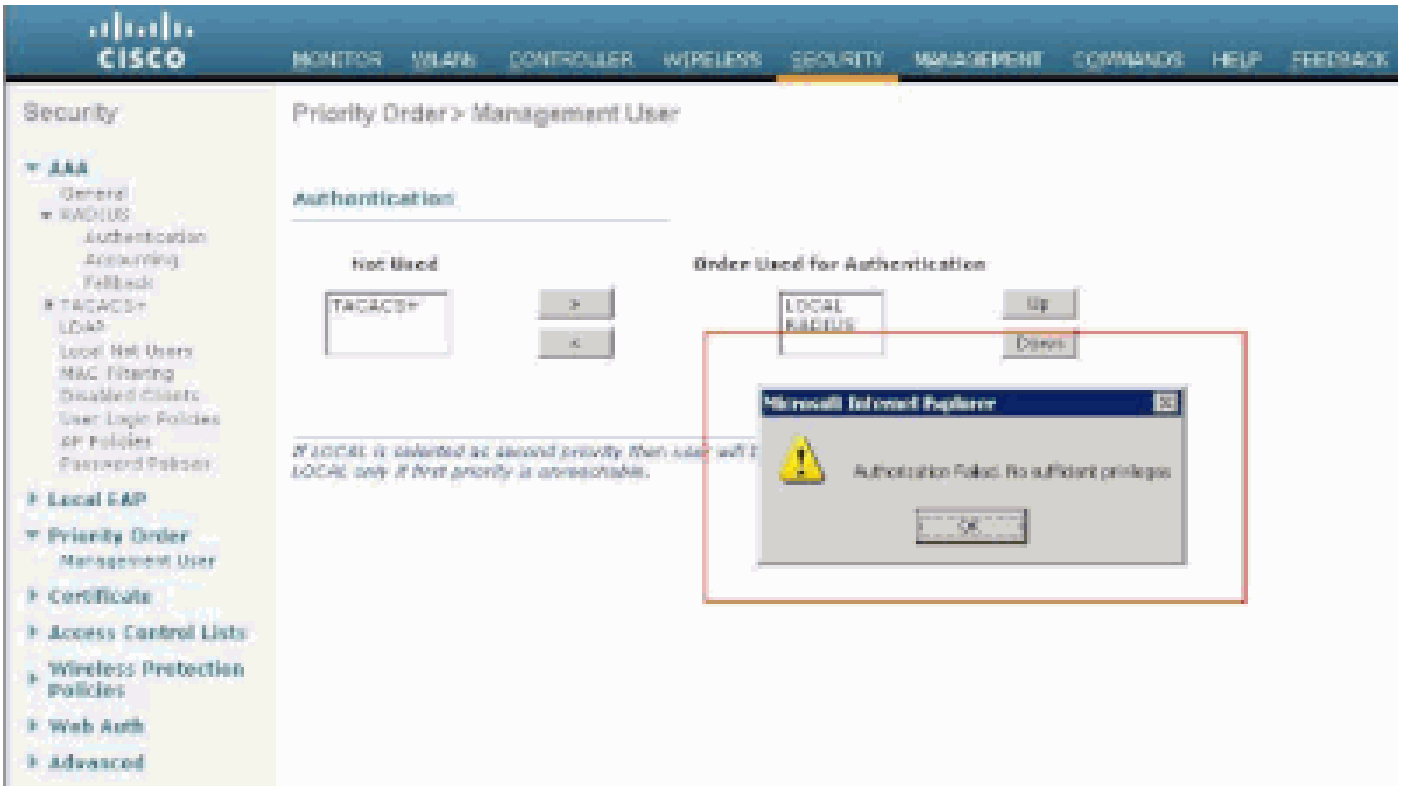
您还可以确保是否为经过身份验证的用户提供ACS指定的访问限制。为此，请通过HTTP/HTTPS访问WLC GUI（确保WLC配置为允许HTTP/HTTPS）。

在ACS中设置读写访问权限的用户在WLC中具有多个可配置权限。例如，读写用户有权在WLC的WLAN页面下创建新的WLAN。此窗口显示了一个示例。



WLC中的可配置权限

当具有只读权限的用户尝试更改控制器上的配置时，用户会看到此消息。

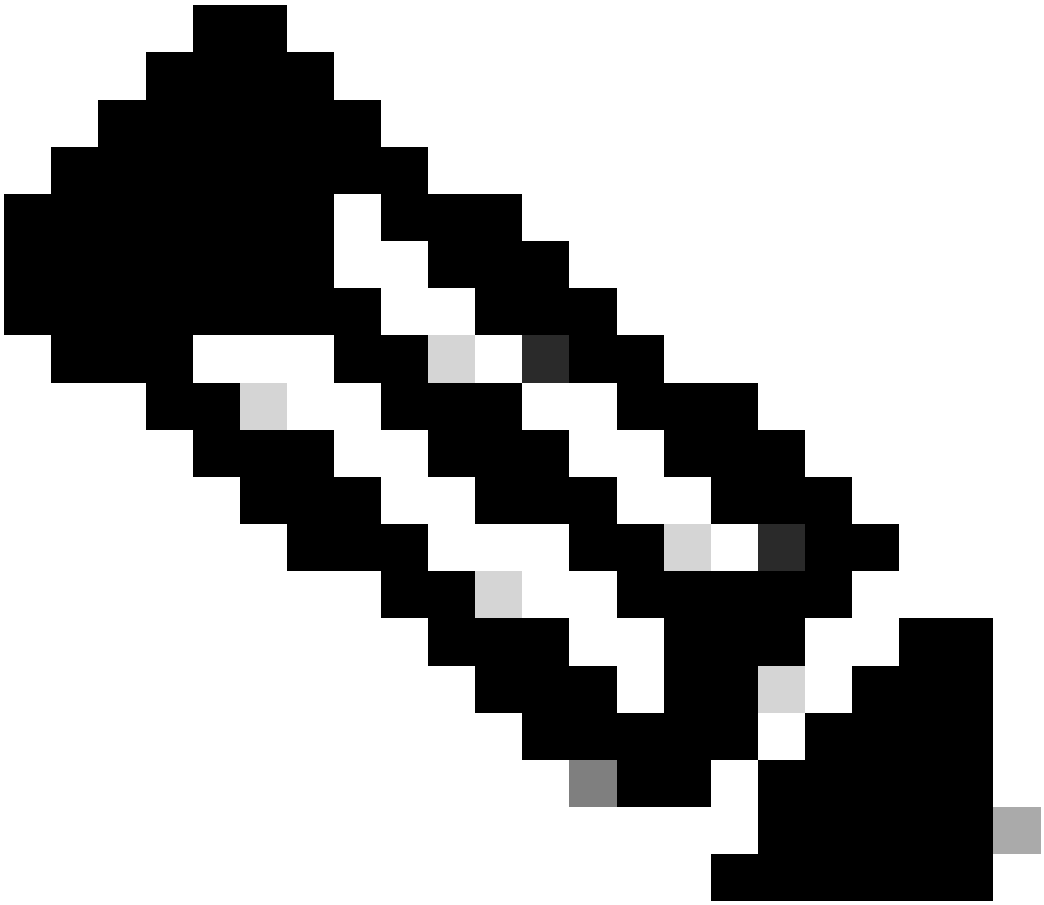


无法更改具有只读访问权限的控制器

这些访问限制也可以通过WLC的CLI进行验证。下面是一个输出示例。

```
<#root>

(Cisco Controller) >

?


debug           Manages system debug options.
help            Help
linktest        Perform a link test to a specified MAC address.
logout          Exit this session. Any unsaved changes are lost.
show            Display switch options and settings.

(Cisco Controller) >config

Incorrect usage.  Use the '?' or <TAB> key to list commands.
```

如本示例输出所示，控制器CLI中的？会显示当前用户可用的命令列表。另请注意，**config** 命令在此示例输出中不可用。这说明只读用户没有权限在WLC上执行任何配置。但是，读写用户拥有在控制器上执行配置的权限（GUI和CLI模式）。



注意：即使您通过RADIUS服务器对WLC用户进行了身份验证（当您逐页浏览时），HTTP[S]服务器仍会每次都对客户端进行完全身份验证。未在每个页面上提示您进行身份验证的唯一原因是您的浏览器缓存并重播您的凭证。

故障排除

在某些情况下，控制器通过ACS对管理用户进行身份验证，身份验证成功完成(access-accept)，并且在控制器上看不到任何授权错误。但是，系统再次提示用户进行身份验证。

在这些情况下，您无法解释错误以及用户为什么不能仅使用**debug aaa events enable** 命令登录到WLC中。相反，控制器会显示另一个身份验证提示。

出现这种情况的一个可能原因是，ACS未配置为传输该特定用户或组的Service-Type属性，即使ACS上正确配置了用户名和密码。

debug aaa events enable

命令的输出并不表明用户没有所需的属性（例如，Service-Type属性），即使**access-accept**从AAA服务器发送回也是如此。**debug aaa events enable** 示例命令输出显示一个示例。

```
<#root>

 (Cisco Controller) >


debug aaa events enable

Mon Aug 13 20:14:33 2011: AuthenticationRequest: 0xa449a8c

Mon Aug 13 20:14:33 2011: Callback.....................................0x8250c40

Mon Aug 13 20:14:33 2011: protocolType.................................0x00020001

Mon Aug 13 20:14:33 2011: proxyState.....................1A:00:00:00:00:00-00:00

Mon Aug 13 20:14:33 2011: Packet contains 5 AVPs (not shown)

Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Successful transmission of
Authentication Packet (id 8) to 172.16.1.1:1812, proxy state
1a:00:00:00:00:00-00:00

Mon Aug 13 20:14:33 2011: ****Enter processIncomingMessages: response code=2

Mon Aug 13 20:14:33 2011: ****Enter processRadiusResponse: response code=2

Mon Aug 13 20:14:33 2011: 1a:00:00:00:00:00 Access-Accept
received from RADIUS server 172.16.1.1 for mobile 1a:00:00:00:00:00 receiveId = 0
```

```
Mon Aug 13 20:14:33 2011: AuthorizationResponse: 0x9802520

Mon Aug 13 20:14:33 2011: structureSize.............................28

Mon Aug 13 20:14:33 2011: resultCode.................................0

Mon Aug 13 20:14:33 2011: protocolUsed.............................0x00000001

Mon Aug 13 20:14:33 2011: proxyState......................1A:00:00:00:00:00-00:00

Mon Aug 13 20:14:33 2011: Packet contains 0 AVPs:
```

在此第一个示例**debug aaa events enable** 命令输出中，您看到Access-Accept已成功从RADIUS服务器接收，但Service-Type属性未传递到WLC。这是因为ACS上没有使用此属性配置特定用户。

需要将Cisco Secure ACS配置为在用户身份验证后返回Service-Type属性。必须根据用户权限将Service-Type属性值设置为**Administrative**或**NAS-Prompt**。

第二个示例再次显示**debug aaa events enable**命令输出。但是，这次ACS上的Service-Type属性设置为**Administrative**。

```
    <#root>

(Cisco Controller)>

debug aaa events enable
```

```
Mon Aug 13 20:17:02 2011: AuthenticationRequest: 0xa449f1c

Mon Aug 13 20:17:02 2011: Callback.................................0x8250c40

Mon Aug 13 20:17:02 2011: protocolType.............................0x00020001

Mon Aug 13 20:17:02 2011: proxyState......................1D:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: Packet contains 5 AVPs (not shown)
```

```
Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Successful transmission of
Authentication Packet (id 11) to 172.16.1.1:1812, proxy state
1d:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: ****Enter processIncomingMessages: response code=2

Mon Aug 13 20:17:02 2011: ****Enter processRadiusResponse: response code=2
```

Mon Aug 13 20:17:02 2011: 1d:00:00:00:00:00 Access-Accept received from RADIUS server 172.16.1.1 for mobile 1d:00:00:00:00:00 receiveId = 0

```
Mon Aug 13 20:17:02 2011: AuthorizationResponse: 0x9802520

Mon Aug 13 20:17:02 2011: structureSize.............................100

Mon Aug 13 20:17:02 2011: resultCode.................................0

Mon Aug 13 20:17:02 2011: protocolUsed.............................0x00000001

Mon Aug 13 20:17:02 2011: proxyState......................1D:00:00:00:00:00-00:00

Mon Aug 13 20:17:02 2011: Packet contains 2 AVPs:
```

Mon Aug 13 20:17:02 2011: AVP[01] Service-Type..........0x00000006 (6) (4 bytes)

```
Mon Aug 13 20:17:02 2011: AVP[02] Class.........
CISCOACS:000d1b9f/ac100128/acsserver (36 bytes)
```

在前面的示例输出中，您可以看到Service-Type属性已传递到WLC。

相关信息

- 配置无线LAN控制器-配置指南
- 在无线局域网控制器上配置VLAN
- 配置RADIUS服务器和WLC进行动态VLAN分配
- 无线局域网控制器和轻量级无线接入点的基本配置
- 使用无线局域网控制器配置AP组VLAN
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。